AMENDMENTS TO THE CLAIMS

The following is a complete and revised listing of the claims, marked with status identifiers in parentheses, underlines indicating insertions, and strikethroughs or double brackets indicating deletions. This listing is to replace all prior listing of the claims:

LISTING OF CLAIMS

1. (previously presented) A method of validating a user for a transaction to be effectuated by using a transaction card, comprising:

configuring a biometric profile for said user, said biometric profile including a plurality of biometric samples received from the user, the plurality of biometric samples corresponding to a plurality of questions;

associating said biometric profile with an indicium assigned to said transaction card;

biometrically interrogating said user when said transaction is attempted by said user, wherein said biometrical interrogation includes querying said user for a biometric response associated with a randomly selected one of said plurality of questions;

monitoring said biometric response generated with respect to said user in response to the biometrical interrogation;

determining if said biometric response matches a biometric sample in said biometric profile corresponding to the randomly selected one of said plurality of questions; and

if so, approving said user for said transaction.

2. (previously presented) The method of validating a user for a transaction as set forth in claim 1, wherein at least a portion of said plurality of biometric samples comprises voice samples generated by said user responsive to a plurality of questions directed to said user in said configuring step, and further wherein said biometrical interrogation involves querying said user for a voice response to a randomly selected question of said plurality of questions.

3. (previously presented) The method of validating a user for a transaction as set forth in claim 1, further comprising:

prompting said user to input said indicium assigned to said transaction card after determining that said biometric response matches a biometric sample of said biometric profile;

determining if said indicium is a valid personal identification number operating as a password associated with said transaction card; and

denying access to said user for said transaction if said indicium is not a valid personal identification number associated with said transaction card.

4. (previously presented) The method of validating a user for a transaction as set forth in claim 1, further comprising:

prompting said user to input said indicium assigned to said transaction card if said biometric response does not match a biometric sample of said biometric profile;

confirming that said indicium is a valid personal identification number associated

with said transaction card; and

approving said user for said transaction upon said confirmation.

5. (previously presented) The method of validating a user for a transaction as set forth in claim 1, wherein configuring a biometric profile for said user is effectuated manually.

6. (previously presented) The method of validating a user for a transaction as set forth in claim 1, wherein configuring a biometric profile for said user is effectuated automatically.

7. (previously presented) The method of validating a user for a transaction as set forth in claim 1, further comprising updating said biometric profile for said user.

8. (previously presented) A method of validating a user for a call to be effectuated over a Public Switched Telephone Network (PSTN) using a calling card, comprising:

configuring a personalized profile for said user, said personalized profile including a plurality of voice samples elicited from said user in response to a plurality of personalized questions directed to said user;

associating said personalized profile with an indicium assigned to said calling card;

determining if a voice verification is needed with respect to said user when said call is attempted by said user;

if so, querying said user for a voice response to a question that is randomly

selected from said plurality of personalized questions;

verifying if said voice response matches a corresponding voice sample in said voice profile; and

if so, approving said user for said call involving said calling card.

9. (previously presented) The method of validating a user for a call as set forth in claim 8, further comprising:

populating at least a portion of said personalized profile with a plurality of Dual Tone Multi Frequency (DTMF) sample responses elicited from said user in said configuration step;

prompting said user to input a DTMF response in response to said question that is randomly selected from said plurality of personalized questions;

verifying if said DTMF response matches a corresponding sample response in said personalized profile; and

denying access to said user for said call if said DTMF response does not match said corresponding sample response in said personalized profile.

10. (previously presented) The method of validating a user for a call as set forth in claim 8, further comprising:

prompting said user to input said indicium assigned to said calling card after verifying that said voice response matches a corresponding voice sample in said voice profile;

determining if said indicium is a valid personal identification number associated

with said calling card; and

denying access to said user for said call if said indicium is not a valid personal identification number associated with said calling card.

11. (previously presented) The method of validating a user for a call as set forth in claim 8, further comprising:

prompting said user to input said indicium assigned to said calling card after verifying that said voice response does not match a corresponding voice sample in said voice profile;

confirming that said indicium is a valid personal identification number associated with said calling card; and

approving said user for said call upon said confirmation.

12-15. (canceled).

16. (previously presented) An access control system for use with a transaction-card-based scheme, said system comprising:

a network operable with a terminal, said terminal for interacting with a user in association with a transaction card;

a controller disposed in the network to query said user when said user attempts a transaction using said transaction card;

a server disposed in the network, said server responding to messages from said controller with respect to querying said user; and

a profile database coupled to said server, said profile database having a plurality of biometric samples inherently coupled to said user, wherein said plurality of biometric samples relate to a plurality of questions, and wherein said biometric samples are associated with an indicium assigned to said transaction card such that when said user attempts said transaction, said controller queries said user for a response relating to a randomly selected one of the biometric samples and if said response does not match a corresponding entry in said profile database, access is denied to said user for said transaction.

17. (original) The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said entry inherently coupled to said user comprises at least one of a fingerprint, retinal scan, palm print, and implanted ID chip associated with said user.

18. (original) The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said entry inherently coupled to said user comprises a voiceprint associated with said user.

19. (original) The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said controller comprises an Automated Response Unit associated with a Public Switched Telephone Network.

20. (original) The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said terminal comprises a wireline phone.

21. (original) The access control system for use with a transaction-card based scheme as set forth in claim 16, wherein said terminal comprises an Internet phone.

22. (original) The access control system for use with a transaction-card-based scheme as set forth in claim 16, wherein said terminal comprises a wireless medium device.